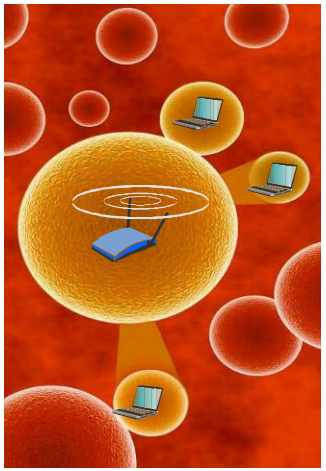
Wi-Fish Finder: Who will bite the bait?

There is >50 % chance that your laptop will!

Md Sohail Ahmad
Prabhash Dhyani
AirTight Networks
www.airtightnetworks.com

AirTight® NETWORKS

About the Speaker



- Last year brought to you Autoimmunity Disorder in Wireless LANs at Defcon 16

  http://www.defcon.org/html/defcon-16/dc-16-speakers.html#Ahmad

- The year before served you Caffe Latte at Toorcon 9

  http://www.toorcon.org/2007/event.php?id=25

AirTight® NETWORKS

What Motivated This Presentation

- A lot has been written and said about dangers of using OPEN and WEP based WiFi networks
- Yet, level of awareness about WiFi vulnerabilities is still very low. A recent study by AirTight Networks in April 2009
  http://www.airtightnetworks.com/home/resources/knowledge-center/financial-districts-scanning-report.html
  - 56 % Clients were found to be probing for one or more SSIDs
  - 13 % Clients were found probing for OPEN ad hoc networks

Most users are vulnerable, yet they are unaware

Perhaps Showing Them a Mirror Will Help…

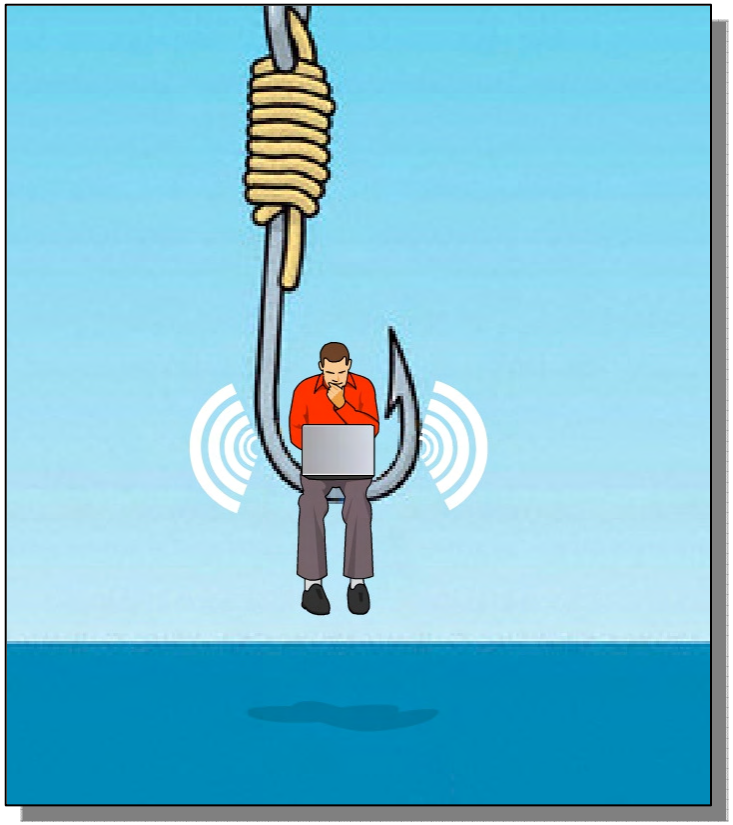
Wi-Fish Finder is a tool for

1. Discovering active WiFi clients
2. Finding networks they are probing for
3. Finding security settings of the probed network

1,2 has been done before

What's cool? --- Step 3

What needs attention? – clients which only connect to WPA, WPA2 networks can also be vulnerable!



AirTight® NETWORKS

Network Name Leakage from WiFi Cards

```
0:21:6:48:3a:[illegible]  | UA_WPA, UAlbanyWiFi, NETGEAR, @Home, tmobile
0:21:6:62:5c:[illegible]  | @Home, tmobile
0:21:6:78:47:[illegible]  | VenetianWiFi, default, @Home, tmobile
0:21:6:a6:cb:[illegible]  | Bran Muffin 2009, @Home, tmobile
0:21:6:aa:95:[illegible]  | @Home, tmobile
0:21:6:b4:cf:[illegible]  | steve, Wayport_Access, mednik-verizon, Image Wireless, prodigymovil, @Home, tmobile
0:21:6:c1:f9:[illegible]  | digis-465, @Home, tmobile, claytons, VDAPL, linksys, AISWIRELESS, tenney sibling network, moabkoa
0:21:6:ca:95:[illegible]  | @Home, tmobile
0:21:6:dc:cf:[illegible]  | @Home, tmobile
0:21:6:e3:48:[illegible]  | @Home, tmobile
0:21:6:eb:45:[illegible]  | tmobile
0:21:6:f0:51:[illegible]  | @Home
0:21:6:f1:31:[illegible]  | @Home, tmobile
0:21:6:f:64:[illegible]   | @Home33D4, @Home
0:21:e9:72:f4:[illegible] | Garbanzo
0:22:41:fc:53:78 | linksys
0:23:4d:9d:db:[illegible] | PAGE, etada, YOUWISH, 911PCTECH-2.4GHz, BRIGHT, GGTO, GGNH, GGLA
0:23:6c:14:92:[illegible] | dlink
0:23:6c:43:15:aa | B20
0:23:7a:26:1a:[illegible] | @Home, tmobile
0:23:7a:4b:6b:[illegible] | attwifi, Regele, WESTIN-GUEST, default, Washington Dulles WiFi
0:23:7a:4b:8a:[illegible] | attwifi, JetBlue Hotspot
0:23:7a:51:71:[illegible] | attwifi, linksys
0:23:7a:51:95:[illegible] | attwifi
0:23:7a:5f:7:[illegible]  | @Home, tmobile
0:23:7a:60:85:d6 | @Home, tmobile
0:23:7a:67:7f:[illegible] | @Home, tmobile
0:23:7a:71:12:[illegible] | Sala_Productores, JET-ARRIBA, default, NegroNet, lapccs-2, WLAN_74
```

WiFi enabled roaming clients normally leak the name of the networks they have been connecting to in the past

- Some of these networks could be Open or WEP and leaves client vulnerable to Honeypot style attacks

AirTight® NETWORKS

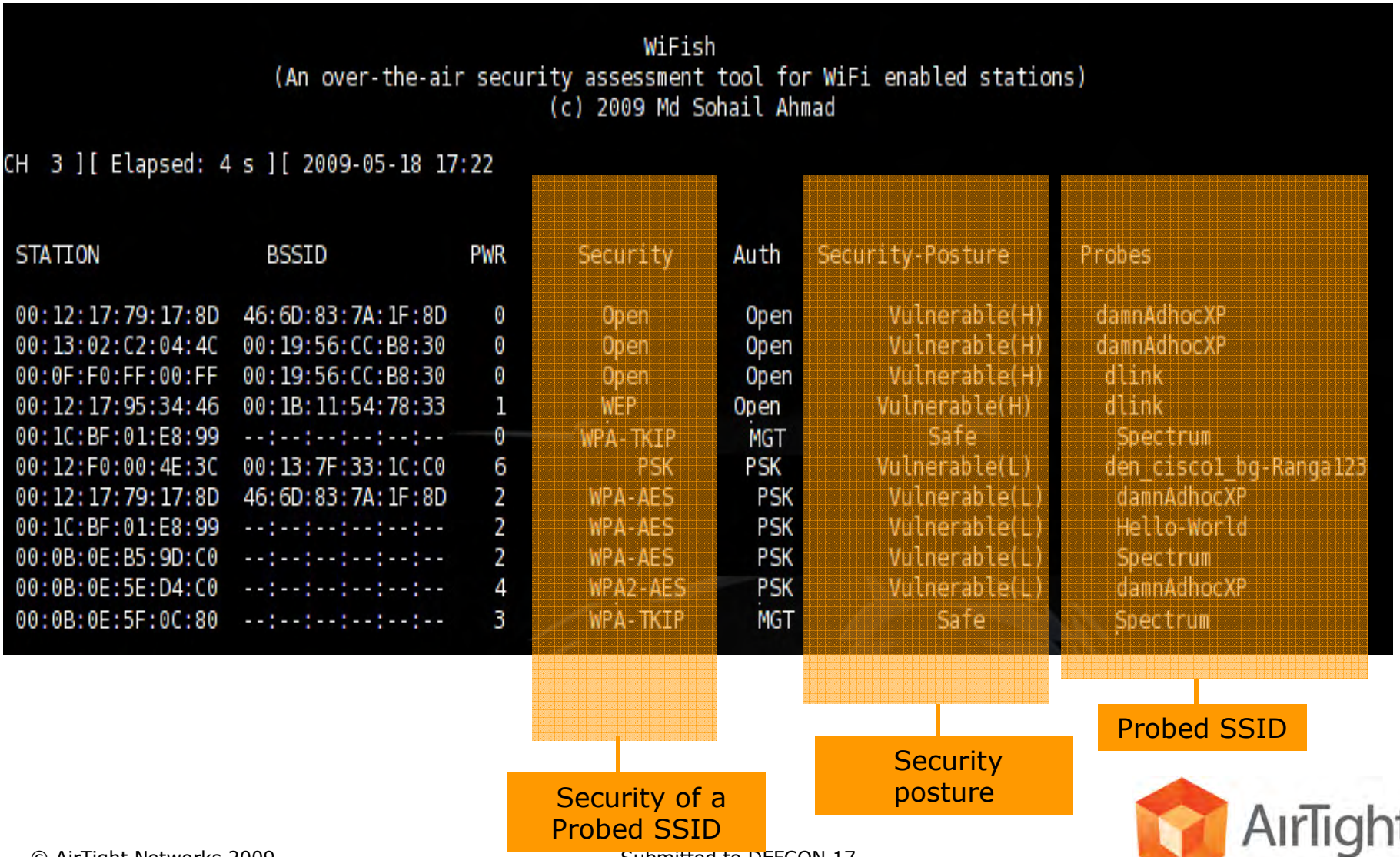
Can Security Mode of Each Probed Network (OPEN, WEP, WPA or WPA2) be Determined?

WiFi enabled laptop keeps memory of various WiFi networks it has connected to in the past

If correct security setting of each probed SSID can be determined then a matching honeypot can be instantly created!

AirTight® NETWORKS

Yes, it is possible!



How?

We will discuss details of Wi-Fish Finder during presentation

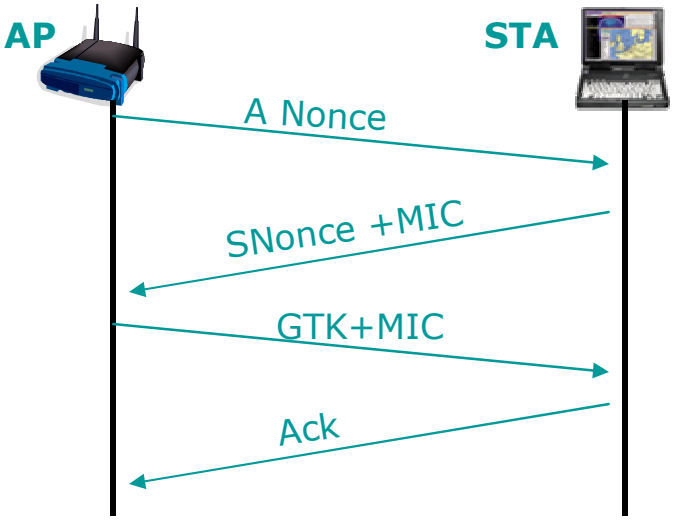
We will also do a Live Demo of Wi-Fish Finder

AirTight® NETWORKS

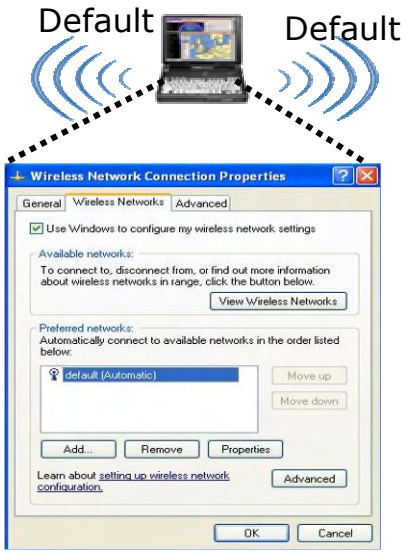
Important Points

- If the probed SSID list contains at least one OPEN network
  - A simple OPEN honeypot will do the trick
- Else, if the probed SSID list containst at least one WEP network
  - Caffe Latte will do the trick
- Else, if the probed SSID list contains only WPA-PSK networks
  - Honeypot attack still possible! (see the next slide)
- Else, if the probed SSID list contains only WPA2 network
  - Honeypot attack still possible in some cases (see the next slide)

The Latest Advancement In Dictionary Attack Tool



4-Way Handshake

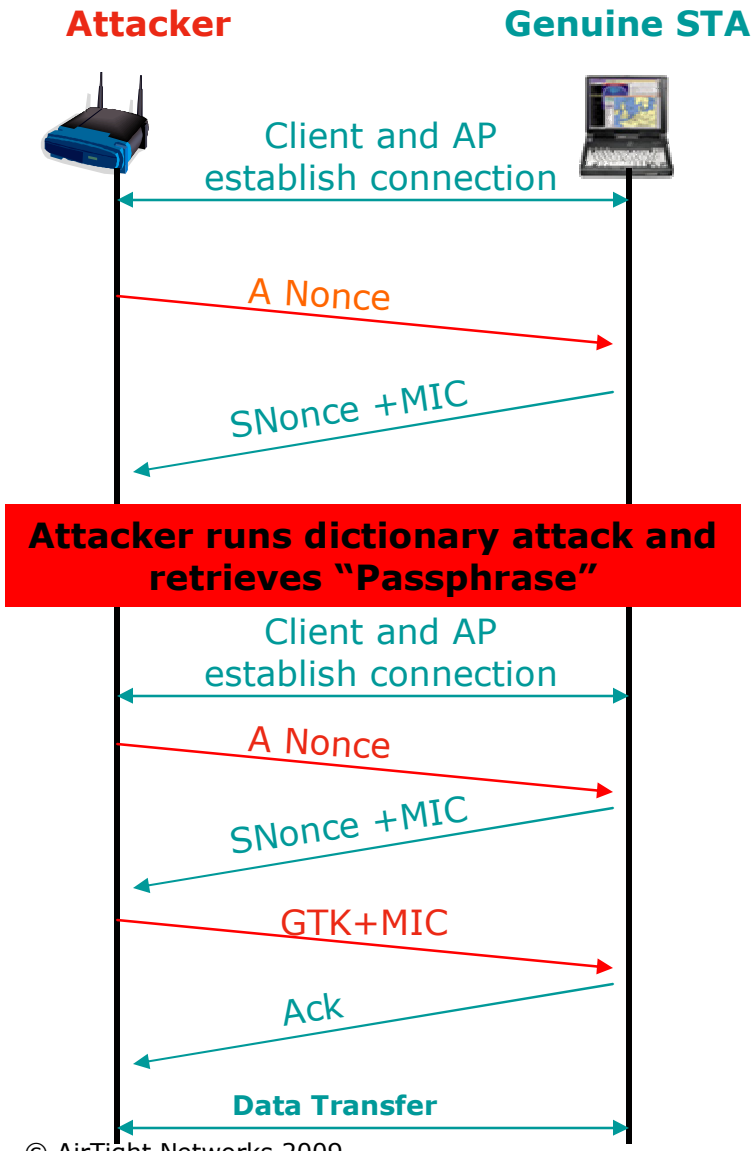


- To run dictionary attack all we need is 4 way EAPOL handshake packets
  - Thanks to Thomas D'Otreppe latest aircrak-ng doesn't require all 4 handshake frames
  - Disclosure in UNAM, Mexico City November 27-28, 2008

- Windows caches the Passphrase or Pre-Shared Key of networks in its PNL

AirTight® NETWORKS

WPA/WPA2-PSK Clients can be targeted: Attack Choreography



- Attacker collects first two frames of 4-way handshake by setting-up a fake access point and luring client to connect to it
- Passphrase is retrieved by launching dictionary attack using latest aircrack-ng tool
- AP is again configured with correct Passphrashe (PSK)
- This time client is successfully able to complete the 4-way handshake
- Client machine now gets connected to attacker's machine

AirTight® NETWORKS

Conclusion

- While lot of measures have been taken to secure WiFi infrastructure (both APs and Client in the vicinity) by following best practices and deploying various forms of WIPS solution, WiFi enabled devices are still need adequate security cover
- An infected laptop can be serious security threat to an organization as it can lead to an attack, recently, uncovered by SANS

  Newest WLAN Hacks Come From Afar

  http://darkreading.com/security/vulnerabilities/showArticle.jhtml;jsessionid=2Y42ER3MPBL2OQSNDLOSKHSCJUNN2JVN?articleID=217100332
- WiFish Finder is a perfect tool to reflect the security posture of a WiFi enabled client devices and could be used to assess their security risk level

AirTight® NETWORKS

…Food For Thought

Hidden SSID of an Access Point can be discovered in a matter of seconds

If a client is not broadcasting SSID in probes
Can it's PNL be guessed !

Hint: Dictionary Attack !

AirTight® NETWORKS

Questions?

Md Sohail Ahmad
md.ahmad@airtightnetworks.com
sohail_alig@yahoo.com

Prabhash Dhyani
prabhash.dhyani@airtightnetworks.com

AirTight Networks
www.airtightnetworks.com